UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

CHRISTOPHER GEORGE PABLE, *Plaintiff*, v. CHICAGO TRANSIT AUTHORITY and CLEVER DEVICES LTD., *Defendants*.	Case No. 19-cv-7868 Judge Elaine E. Bucklo
CHICAGO TRANSIT AUTHORITY, *Counter-Plaintiff*, v. CHRISTOPHER GEORGE PABLE, *Counter-Defendant*.	

CHICAGO TRANSIT AUTHORITY'S MOTION TO COMPEL PLAINTIFF TO PRODUCE HIS CELL PHONE FOR INSPECTION AND IMAGING AND RESPOND TO THE CTA'S REQUEST FOR PRODUCTION

Dated: February 5, 2021

Respectfully submitted,

CHICAGO TRANSIT AUTHORITY

By: *s/ Elizabeth E. Babbitt*
One of Its Attorneys

John F. Kennedy
jkennedy@taftlaw.com
Elizabeth E. Babbitt
ebabbitt@taftlaw.com
Allison E. Czerniak
aczerniak@taftlaw.com
Nicollette L. Khuans
nkhuans@taftlaw.com
TAFT STETTINIUS & HOLLISTER LLP
111 East Wacker, Suite 2800
Chicago, Illinois 60601
(312) 527-4000

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Rules

INTRODUCTION

The CTA's efforts to obtain from Plaintiff relevant information relating to the claims and counterclaims asserted in this matter have been unfairly hindered by Plaintiff's evasive and dilatory discovery responses. Most recently, on October 31, 2020, Plaintiff produced an image of his personal cell phone that he used during the relevant time period, which the CTA has requested since March 2020, and which Plaintiff imaged on June 11, 2020. Plaintiff's image of the phone is effectively an empty box. According to Plaintiff, while his personal cell phone was in his sole custody, the CTA allegedly caused his phone to be wiped clean and deleted all of Plaintiff's personal data when the CTA terminated Plaintiff's access to the CTA network system and server upon his termination of employment. Plaintiff refuses to turn over the cell phone so the CTA can complete a forensic analysis.

The cell phone also seems to have suffered additional harm while in Plaintiff's sole custody. Plaintiff told the CTA that sometime after he imaged the cell phone on June 11, 2020, but *before* the image was actually produced to the CTA, the cell phone may have become inoperable. The CTA's forensic expert should be allowed to examine and image Plaintiff's cell phone, and the CTA requests an Order compelling Plaintiff to do so. The CTA's concerns with Plaintiff's handling of his phone are compounded by the fact that Plaintiff is a self-proclaimed hacking expert and an extremely sophisticated computer technician with expertise in developing and modifying computer code, and in the management of computer systems, IT security, and encryption.

Plaintiff's phone is material to this case for two reasons. First, Plaintiff failed to produce relevant communications that the CTA knows exist (confirmed through other discovery)—despite the CTA's many requests for these materials. Particularly in light of Plaintiff's expertise, his failure to produce communications known to exist raises spoliation concerns. The CTA believes evidence of these communications may continue to exist on the phone.

Second, Plaintiff's cell phone, itself, is also directly at issue in this litigation and is an instrument of Plaintiff's unlawful conduct. The CTA contends in its counterclaim that Plaintiff encrypted his CTA computer without authorization, rendering the computer inaccessible upon his departure from the CTA, in violation of the Computer Fraud & Abuse Act ("CFAA"), 18 U.S.C. § 1030, *et seq*. Plaintiff, for his part, asserts that when the CTA allegedly remotely wiped Plaintiff's cell phone following his departure from the CTA, this in turn rendered Plaintiff's CTA computer inaccessible. In asserting this defense, Plaintiff places his cell phone directly at issue in this matter. Indeed, Plaintiff does not (and cannot) contest the clear relevance of this evidence, given that he has already agreed to produce a complete image of his phone.

The CTA detailed Plaintiff's discovery deficiencies through Local Rule 37.2 communications. Yet, Plaintiff refuses to provide his phone and its relevant component parts to be inspected and re-imaged to enable the CTA to obtain a complete forensic image. It is possible that if the phone is not re-imaged in an appropriate manner consistent with industry standards, relevant evidence will be lost (if it has not been lost already).

The CTA's spoliation concerns are further exacerbated by Plaintiff's recent conduct relating to his personal website. In the course of its investigation into Plaintiff's claims and its counterclaim, the CTA discovered that Plaintiff's personal website, www.menchi.org, contained detailed and proprietary information about certain CTA technology projects. The CTA captured screenshots of this information on Plaintiff's website on or about October 15, 2020. Since that date, Plaintiff has deleted that information and refuses to produce it, despite his discovery obligations. The CTA seeks to assess the scope and extent of its proprietary information shared by Plaintiff in the public domain, as it raises security concerns and may lead to other relevant evidence

in the case. Plaintiff has refused to provide these relevant materials in response to the CTA's discovery requests.

Plaintiff, like all litigants, has a duty to preserve any and all materials that are relevant to any party's claims or defenses. That duty has existed since Plaintiff had notice of his claims in 2018. Because Plaintiff has failed to fulfill his discovery obligations, the CTA respectfully asks the Court to compel him to do so.

BACKGROUND

I. Plaintiff's cell phone is directly relevant to the CTA's affirmative defenses and its counterclaim against Plaintiff.

Plaintiff resigned in lieu of termination from the CTA on November 8, 2018 after an internal investigation at the CTA revealed that Plaintiff and his supervisor, Michael Haynes ("Haynes"), had used a "Skeleton Key" they had discovered in BusTime, an application created by Clever Devices and used by the CTA to provide service information to public transit users, to hack into the BusTime application of other metro transit systems. In one instance, Plaintiff and Haynes's use of the Skeleton Key caused an outdated and inaccurate tweet to reissue on the Dayton Regional Transit Authority's ("Dayton RTA") Twitter account. Only then did Plaintiff and Haynes reveal their actions, first to Dayton RTA, and then to Clever Devices. Plaintiff continued, however, to conceal his conduct from CTA management. In fact, the CTA did not learn of the full extent of Plaintiff's misdeeds until it received a letter from Clever Devices on October 22, 2018, detailing the misconduct and threatening legal action against the CTA. After a thorough investigation of the matter, the CTA determined that Plaintiff violated multiple CTA rules, policies, and procedures that warranted his termination. Plaintiff resigned in lieu of termination.

Thereafter, Plaintiff filed a single-count complaint against the CTA and Clever Devices on December 2, 2019, alleging a whistleblower claim under the National Transit Systems Security

Act ("NTSSA"). (Dkt. 1.) Plaintiff claims that he engaged in protected activity under the NTSSA by discovering and reporting the Skeleton Key, which he asserts was a "serious security flaw" in the BusTime application. In response to Plaintiff's claim, which the CTA denies, the CTA has alleged certain affirmative defenses, including, as relevant here, that the CTA would have taken the same personnel action in the absence of the alleged protected activity due to Plaintiff's other misconduct and unclean hands. (Dkts. 8, 30.)

The CTA also filed a counterclaim against Plaintiff under the CFAA relating to the same transactions or occurrences that are the subject matter of Plaintiff's complaint, as well as Plaintiff's unauthorized use and encryption of the CTA computer he used during the course of his employment. (Dkt. 32.) The CTA alleged that Plaintiff created and applied password(s) to encrypt his CTA computer at various points of access without the CTA's authorization or knowledge, including through the use of encryption applications installed on his personal cell phone, depriving the CTA of its ability to access its own computer following Plaintiff's departure from the CTA. (*Id*.) Plaintiff asserts in response that "[a]ny inability or other difficulties associated with accessing data on Pable's computer is the direct result of the CTA's conduct . . . the CTA's unilateral decision, with no notice or warning to Pable, to disable access to certain data stored on Pable's phone, eliminated the ability to access the encrypted data on the Computer." (Dkt. 34.)

The information contained on Plaintiff's phone is directly relevant to the issues raised by the CTA's affirmative defenses to Plaintiff's claim, as it may contain communications regarding Plaintiff's discovery and use of the Skeleton Key on other transit systems, including Dayton RTA. Likewise, the phone is directly at issue on the CTA's counterclaim—as made apparent by Plaintiff's asserted defense to the encryption claim. Plaintiff, himself, acknowledges that evidence relating to the encryption of CTA computer is contained on his phone.

A. The CTA has sought the preservation, imaging and forensic inspection of Plaintiff's cell phone from the outset of this litigation.

On March 2, 2020, the Parties filed their Mandatory Initial Discovery Pilot Program ("MIDPP") initial disclosures. (*See* Dkts. 14, 15 and 16.) The CTA identified various deficiencies in Plaintiff's initial MIDPP production, which the Parties discussed during two Rule 26 teleconferences (the "March Teleconferences"). The CTA further detailed these deficiencies in Rule 37.2 correspondence. (*See* March 18, 2020 Rule 37.2 Letter from E. Babbitt, attached hereto as Exhibit A.) The CTA noted that Plaintiff's production referenced the existence of relevant text messages that had not been produced and the CTA requested that the cell phone Plaintiff used in 2018 during the time of his employment at the CTA[1] be preserved and imaged by a third-party vendor for production to the CTA.

In response, Plaintiff agreed to supplement his ESI production, but refused to have his cell phone imaged. (*See* March 25, 2020 Rule 37.2 Letter from T. Duffy, attached hereto as Exhibit B.) Plaintiff indicated that the CTA "disabled all access to [Plaintiff's] cell phone data" and, in doing so, prevented Plaintiff from accessing his password storage application, Moto Key, which allegedly contained the information necessary to access Plaintiff's computer at the CTA. (*Id.*) In other words, Plaintiff claimed that when the CTA terminated his access to his CTA email and the CTA network, this termination triggered a complete disabling or deletion of the contents of Plaintiff's personal cell phone—a claim that defies logic and is not supported by the facts.[2]

---

[1] Plaintiff has represented to the CTA that he used a single personal cell phone during the relevant time period. As a result, the discovery efforts have focused on that device, despite the CTA's initial request for relevant information pertaining to *any* devices used by Plaintiff in 2018.

[2] The CTA does not provide support for or otherwise maintain access to its employees' personal cell phones, such as Plaintiff's phone at issue here. When a CTA employee resigns or is terminated, the CTA will disable the employee's access to the CTA network and the employee's CTA email account. The CTA takes no further steps to "wipe," delete, or otherwise disable information stored on an employee's personal phone upon termination.

The Parties filed their Joint Initial Planning Report pursuant to Rule 26(f) and their obligations under the MIDPP on June 18, 2020. (Dkt. 27.) That Report memorialized the Parties' obligations under the MIDPP to produce all of the ESI identified in their MIDPP initial disclosures by June 29, 2020. (*Id.* at 7.) While the CTA and Clever Devices each made substantial ESI productions on June 29, 2020, Plaintiff made no production. Plaintiff claimed the initial, deficient production he made satisfied his obligations to produce ESI under the MIDPP by June 29, 2020. (June 17, 2020 Email Correspondence from T. Duffy, attached hereto as Exhibit C.)

The deficiencies in Plaintiff's initial production remained unresolved, despite Plaintiff being on notice of, and agreeing to cure these deficiencies in March 2020. The CTA noted these deficiencies in the Joint Initial Planning Report and stated that if the deficiencies were not corrected, motion practice may become necessary. (Dkt. 27 at 7.) Ultimately, Plaintiff made a supplemental MIDPP production on July 30, 2020, consisting of 2,450 images, including: 252 emails from Plaintiff's personal email account in their native format; an Excel spreadsheet containing only portions of Plaintiff's extracted message threads that were sent and received in the messaging application Google Hangouts, along with accompanying images and videos sent and received by Plaintiff through Google Hangouts; and 73 individual photographs of portions of Plaintiff's message threads that were sent and received on Plaintiff's cell phone via either Google Hangouts or Signal, an encrypted messaging application.

The photographs produced were a scanned PDF of photographs taken by an individual holding Plaintiff's phone, depicting various portions of messages on the phone screen:

Obviously, a photograph of a text message in a PDF document such as the one above does not provide the viewer with any relevant metadata, including the times and dates of the messages sent, and the identity of the corresponding parties.

The CTA identified this and other deficiencies with Plaintiff's production in its September 23, 2020 motion to extend the close of written discovery (Dkt. 36), and its October 13, 2020 Local Rule 37.2 letter to Plaintiff. (*See* October 13, 2020 Rule 37.2 Letter from E. Babbitt, attached hereto as Exhibit D.) For instance, Plaintiff's supplemental production did not include:

- Any messages sent or received by Plaintiff on or before August 17, 2018, by any means, despite the fact that a substantial portion of relevant events occurred on or before August 17, 2018 (the date upon which Plaintiff used the Skeleton Key to access the Dayton RTA BusTime system);
- *Any* text messages, in any format, despite the CTA specifically alerting Plaintiff that his initial MIDPP production failed to include any text messages relative to this

litigation in both of the Rule 26 teleconferences and in its Rule 37.2 letter of March 18, 2020, and even though such information undoubtedly exists;[3] or

- Complete message threads exchanged in the Signal application, and the messages produced were not in their native format as the CTA requested, rendering it impossible for CTA to determine the dates and times on which the Signal messages were sent. (*Id.*)

Further, the production only included a total of 18 messages exchanged between Plaintiff and Haynes on July 28, 2018 in the Google Hangouts application, even though Haynes and Plaintiff frequently communicated with one another via various communication platforms regarding topics relevant to this litigation.[4]

In its October 13, 2020 37.2 Letter to Plaintiff, the CTA noted that all these production deficiencies gave rise to the CTA's concerns surrounding spoliation of evidence, deficient search protocols, and Plaintiff's persistent failure to produce materials that are relevant to this litigation. (*Id.*) The CTA again requested that Plaintiff produce a complete image of his cell phone in order to ensure that all responsive information on the device was discovered and produced.

B. Plaintiff's deficient discovery responses failed to cure his incomplete MIDPP disclosures pertaining to his cell phone.

Two days later, on October 15, 2020, Plaintiff tendered his responses to the CTA's First Requests for Production ("RFPs"). (Plaintiff's October 15, 2020 written Responses to the CTA's

[3] The CTA's Rule 37.2 letter specifically noted Plaintiff's production of an August 24, 2018 email sent by Haynes to his wife and Plaintiff that discusses whether Haynes and Plaintiff should inform the CTA of the unauthorized use of the Skeleton Key on the Dayton RTA BusTime System wherein Haynes writes, "(Just got your text Chris…)." (Ex. A at 1.) Despite this reference to an August 24, 2018 text message from Plaintiff to Haynes regarding the facts at the heart of this litigation, Plaintiff has not produced this, or any other relevant text message.

[4] By way of example, Haynes produced communications exchanged between Haynes and Plaintiff in response to a subpoena the CTA issued to him. Most of these same communications have not been produced by Plaintiff during discovery. For instance, Plaintiff has failed to produce a single text message exchanged between Haynes and Plaintiff, even though these communications undoubtedly exist, as demonstrated by the documents produced by Haynes in response to the CTA's subpoena.

First RFPs, attached hereto as Exhibit E.) The CTA's First RFPs sought relevant communications in their native format, which the CTA expected would be readily available for production as the result of a complete forensic image of Plaintiff's cell phone. (CTA's First RFPs, attached hereto as Exhibit F.) Additionally, the CTA's First RFPs sought "[a]ny and all documents and/or communications showing the compete imaging and/or forensic examination of the personal cell phone(s) that you used during the course of your employment with the CTA in 2018." (*Id*. at Request No. 18.) Plaintiff responded to all of the CTA's First RFPs by objecting or otherwise indicating that all responsive documents were already produced by Plaintiff via his MIDPP disclosures; Plaintiff refused to produce any additional responsive materials. (Ex. E.)

On October 22, 2020, the Parties conducted yet another Local Rule 37.2 teleconference to discuss the deficiencies in Plaintiff's discovery responses. During the call, Plaintiff agreed to produce a complete forensic image file of his personal cell phone, which had been imaged by Plaintiff's third-party expert on June 11, 2020. Plaintiff offered no explanation for the three-month delay in producing the phone image, which the CTA had been requesting since March 2020. Plaintiff indicated that the image may nonetheless be incomplete due to his claim that the CTA "wiped" the cell phone following his departure from the CTA, such that certain information, like text messages, may no longer be available on the device. Plaintiff also informed the CTA for the first time that, at some point after Plaintiff's cell phone was imaged by his third-party expert on June 11, 2020, the cell phone no longer appeared to be operational. Counsel for Plaintiff agreed that Plaintiff would continue to preserve the cell phone. (*See* October 24, 2020 Email Correspondence between E. Babbitt and T. Duffy, attached hereto as Exhibit G.)

C. The image of Plaintiff's cell phone produced by Plaintiff is incomplete; Plaintiff refuses to produce the physical cell phone to the CTA for re-imaging.

On or about October 31, 2020, Plaintiff produced the image of his cell phone.[5] The third-party ESI vendors for both the CTA and Clever Devices were each unable to access the image because the imaging software used by Plaintiff is not commonly used to image cell phones. Thus, on November 17, 2020, the Parties' third-party vendors all participated in a teleconference to troubleshoot the issue. Thereafter, the CTA's third-party vendor was able to access and review the image of Plaintiff's cell phone. This analysis revealed that the image of Plaintiff's cell phone is compromised or otherwise incomplete. (*See* December 2, 2020 Declaration of Nathan Binder, attached hereto as Exhibit H.)

Specifically, the image contains only about .2 GB of user generated data. (*Id.* ¶ 9.) In other words, the reviewable data contained on the image provided by Plaintiff constitutes only .625% of the total capacity of the device. (*Id.*) Further, aside from the call history, the data contained in the image does not predate June 5, 2020—which was six days before the image was taken. (*Id.* ¶ 13.) The scant data contained in the image includes only five (5) irrelevant text messages—despite Haynes having produced relevant text messages he exchanged with Plaintiff during their time of employment with the CTA, and other messages that were exchanged more recently (*i.e.*, after their departure from the CTA). (*Id.* ¶ 10.) The image also does not include any evidence of: (i) communications exchanged on third-party applications, even though the photographs of messages previously produced by Plaintiff indicated that relevant messages were readily available on the

[5] Counsel for Plaintiff has represented that the cell phone image "is a complete image of the data on the phone when the phone was imaged; nothing about the imaging process affected the 'completeness' of the image." (*See* Ex. G.) Said differently, counsel for Plaintiff has not indicated that any portion of the image was withheld for any reason.

cell phone at the time of imaging (*see supra* at 7);[6] (ii) internet browsing and/or search histories; (iii) audio or visual files, including photo images; (iv) information or data associated with 151 of the 200 third-party applications contained on the cell phone; or (v) information or data associated with the cell phone's SD card(s). (Ex. H ¶¶ 10, 12, 13, 15.) Notably, the image contains no indication that the Moto Key application—which Plaintiff claims contained the information necessary to access his computer at the CTA—had ever been installed or utilized on the phone. (*Id.* ¶ 16.) In short, the image produced by Plaintiff is, by Plaintiff's design, an empty box—it is not just devoid of materials relevant to this case, it is devoid of any materials of any substance whatsoever.

The CTA identified these deficiencies in its November 24, 2020 Rule 37.2 Letter to Plaintiff and requested that Plaintiff produce his physical cell phone, along with all affiliated SIM cards, SD cards, and/or devices to the CTA for re-imaging in light of the CTA's concerns. (*See* November 24, 2020 Rule 37.2 Letter from E. Babbitt, attached hereto as Exhibit J.) Inspection and re-imaging of the cell phone and all its component parts is necessary for the CTA to assess the extent to which responsive data exists (or at one time existed) and can be recovered from the device. (Ex. H ¶ 17.)

In response, Plaintiff refuses to produce the cell phone to the CTA for re-imaging. (*See*

---

[6] A comparison of the photographs of Plaintiff's phone, *see, e.g., supra* at 7, against the limited information gleaned from the image of the phone produced by Plaintiff only furthers the CTA's concerns as to the spoliation of evidence, or that Plaintiff is deliberately withholding relevant information from the CTA. Specifically, the image was created on June 11, 2020. (*See* Ex. H ¶ 11.) The photographs of Plaintiff's cell phone, however, were taken on June 12, 2020. (*See* P001346, attached hereto as Exhibit I.) (showing a date of "6 12" in the upper-left corner of the phone screen). If the image of the phone created by Plaintiff on June 11, 2020 was truly accurate and complete as Plaintiff contends, then the image should contain evidence of the messages apparent from the June 12, 2020 photographs—and yet, the image is completely devoid of any evidence of these communications. (Ex. H ¶ 14.)

November 29, 2020 email correspondence from T. Duffy, attached hereto as Exhibit K.) Counsel acknowledged that there is "not much data captured in the images of [Plaintiff's cell phone]," but reiterated Plaintiff's unsubstantiated claim "that a great deal of the data stored on and accessible via the phone was lost when the CTA wiped the device without notice to [Plaintiff]." (*Id.*) The Parties could not resolve the issues in a Rule 37.2 conference held on December 2, 2020.

II. The CTA also seeks complete and accurate copies of Plaintiff's archived personal website.

Separately, the CTA determined during the course of its investigation of this matter that Plaintiff maintains a personal website: www.menchi.org. The CTA produced screenshots from pages on Plaintiff's website that were captured on or about October 15, 2020 during discovery and reveal that the site contained detailed and proprietary information about certain CTA technology projects. Since the CTA captured these images of Plaintiff's website, all information pertaining to the CTA technology projects appears to have been removed from www.menchi.org.

The CTA sought to learn the scope and extent of its proprietary information being shared by Plaintiff because the information being readily available in the public domain implicated security issues. Additionally, the existence of this information on Plaintiff's website may present evidence relating to the CTA's affirmative defenses. Accordingly, on October 29, 2020, the CTA requested complete and accurate archived copies of Plaintiff's personal websites, including but not limited to www.menchi.org, as they appeared from May 1, 2018 through the present. (CTA's Third RFPs, attached hereto as Exhibit L.) Plaintiff objected to the CTA's Third RFPs as "unreasonable, harassing, [and] seek[ing] information not relevant to any party's claim or defense and out of proportion to the needs of the case," and refused to produce any documents in response to the request. (Plaintiff's written Response to CTA's Third RFPs, attached hereto as Exhibit M.)

The CTA addressed Plaintiff's objections in its November 24, 2020 Rule 37.2 Letter. (*See* Ex. J). In response, counsel for Plaintiff indicated that Plaintiff "did not delete any data related to this matter from his website," but that he "has no 'archive' of his website." (*See* Ex. K). During the December 2, 2020 Rule 37.2 teleconference, Plaintiff continued to refuse to produce archived images of his personal website, and maintained that there was nothing, in fact, deleted.

LEGAL STANDARD

Federal Rule of Civil Procedure 26(b)(1) provides, in pertinent part, as follows:

> Unless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit. Information within this scope of discovery need not be admissible in evidence to be discoverable.

Fed. R. Civ. P. 26(b)(1). Rule 34 governs requests for inspection of an opposing party's electronic devices or ESI:

> A party may serve on any other party a request within the scope of Rule 26(b):
>
> (1) to produce and permit the requesting party or its representative to inspect, copy, test, or sample the following items in the responding party's possession, custody, or control:
>
> > (A) any designated documents or electronically stored information—including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations—stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form; or
> >
> > (B) any designated tangible things . . . .

Fed. R. Civ. P. 34. A party may move, pursuant to Rule 37, for an order compelling discovery where the other party's responses are inadequate. Fed. R. Civ. P. 37(a)(3)(B). If the motion is granted, or the requested discovery is provided after the motion is filed, "the court must, after giving an opportunity to be heard, require the party . . . whose conduct necessitated the motion, . . .

or attorney advising that conduct, or both to pay the movant's reasonable expenses incurred in making the motion, including attorney's fees." Fed. R. Civ. P. 37(a)(5)(A).

ARGUMENT

I. The CTA is entitled to inspect and re-image Plaintiff's cell phone.

When determining whether to grant a motion to compel the forensic imaging of a cell phone, courts consider whether the examination will reveal information that is relevant to the claims and defenses in the pending matter and whether it is proportional to the needs of the case given the cell phone owner's compelling privacy interest in the contents of his cell phone. *See, e.g.*, *Belcastro v. United Airlines, Inc.*, 2019 WL 7049914 (N.D. Ill. Dec. 23, 2019); *Hespe v. City of Chicago*, 2016 WL 7240754 (N.D. Ill. Dec. 15, 2016). The CTA's request for inspection and re-imaging of Plaintiff's cell phone easily meets this standard.

A. Plaintiff's cell phone is relevant to the claims and defenses in this litigation and Plaintiff will not be prejudiced by having the phone inspected and re-imaged.

Plaintiff's cell phone contains (or should contain) evidence that is relevant to both the CTA's defenses to Plaintiff's NTSSA claim and the CTA's counterclaim. Specifically, the CTA knows that relevant communications exist between Plaintiff and other third parties regarding Plaintiff's discovery and use of the Skeleton Key—an issue at the heart of his NTSSA claim. Yet these communications have not been produced by Plaintiff. For example, Plaintiff produced relevant emails with Haynes that expressly reference contemporaneous text messages with Haynes, but Plaintiff did not produce those text messages. Similarly, Haynes produced a number of relevant text messages exchanged with Plaintiff, yet Plaintiff has failed to produce this message thread, or *any* other relevant text messages.[7] All of these communications are relevant to Plaintiff's

[7] Plaintiff's duty to preserve and produce relevant evidence "does not change based on defendant['s] other discovery efforts." *Tomasian v. C.D. Peacock, Inc.*, No. 09 C 5665, 2012 WL

actions and impressions in the days immediately surrounding his discovery and use of the Skeleton Key, and Plaintiff—as a party to this litigation—had an independent duty to preserve and produce this relevant evidence. *Webb v. CBS Broad., Inc.*, No. 08 C 6241, 2010 WL 2104179, at *5 (N.D. Ill. May 25, 2010).

Plaintiff's phone is also relevant to the CTA's counterclaim under the CFAA based, in part, on Plaintiff's unauthorized encryption of his CTA computer. Plaintiff's own defense to the CFAA counterclaim puts his phone at issue, by claiming that the CTA somehow "wiped" the cell phone upon Plaintiff's departure from the CTA thereby "disabl[ing] all access to [Plaintiff's] cell phone data," including the Moto Key[8] application, which allegedly contained the information necessary to access the CTA computer used by Plaintiff during the course of his employment. Setting aside the fact that this position strains credulity and lacks any evidentiary support (rather, it is contradicted by the evidence discovered thus far, *see supra* at n.2), it inextricably links Plaintiff's phone to his unauthorized encryption of his CTA computer. Inspecting and creating a *complete* image of Plaintiff's phone, using appropriate industry standards, is necessary for the CTA to provide the CTA with the discovery it requires and is entitled to under the law.

13208522, at *5 (N.D. Ill. Nov. 8, 2012). As the *Tomasian* court explained: "While plaintiff may argue that defendants did not suffer prejudice because the missing emails were cumulative of other evidence produced, this argument does not excuse plaintiff's failure to preserve her sent emails." *Id.* Plaintiff, as a party, "ha[s] an independent obligation to preserve documents relating to [his] claim, and not just those documents that [he] intend[s] to use to support [his] claim. [He] cannot simply piggyback on [the CTA's] discovery efforts." *Webb*, 2010 WL 2104179, at *5.

[8] The image of Plaintiff's cell phone produced by Plaintiff does not contain any data or information pertaining to the Moto Key application, which further suggests that the image is compromised or incomplete. (Ex, H ¶ 16.) If the CTA is unable to reimage the cell phone and review data pertaining to the Moto Key application, then it will be prevented from evaluating relevant information that is critical to its CFAA claim. And, the glaring absence of this information from the image of Plaintiff's cell phone precludes the CTA from defending against Plaintiff's baseless allegations that the CTA remotely wiped the data and information available on Plaintiff's cell phone at the time of his departure from the CTA.

In light of the clear relevance of Plaintiff's cell phone, the CTA's request to inspect and reimage the phone is proportional to the needs of the case and outweighs Plaintiff's privacy interest in the contents of his phone. This is especially true where Plaintiff has *already agreed to produce a complete image* of his cell phone. This is not an overly burdensome request, and Plaintiff will suffer no unfair prejudice from allowing the CTA to inspect and re-image his phone.

The CTA, on the other hand, will be unfairly prejudiced if it is forced to defend against Plaintiff's claim and litigate its CFAA counterclaim without this relevant evidence. If such evidence has been deleted, the CTA is entitled to learn when and how this occurred, and if appropriate, to pursue a spoliation claim against Plaintiff for his failure to preserve relevant evidence. In either event, an inspection and re-imaging of Plaintiff's phone is necessary.

B. The CTA has demonstrated that the image produced by Plaintiff is compromised or incomplete.

A court may also compel a forensic examination of a party's personal devices where the moving party demonstrates that "the responding party has concealed information *or* lacks the expertise necessary to search and retrieve all relevant data." *Belcastro v. United Airlines, Inc.*, 2019 WL 7049914, *2 (N.D. Ill. Dec. 23, 2019). The CTA succeeds on both of these fronts.

The court in *Belcastro* noted, "even if that party has not intentionally withheld discoverable ESI"—which the CTA cannot say with certainty is the case here—a forensic examination of a personal device "may be appropriate when the [] party fails to initiate a reasonable process to search for, collect and produce responsive ESI." *Id.* (internal quotation and citation omitted). As detailed above, the CTA has demonstrated that Plaintiff has failed in his obligation to search and produce relevant information, including communications, like text messages and messages sent via either Google Hangouts or Signal, which the CTA *knows* exist or should have at one point. (*See supra* at 11-12; Ex. H.) For instance, the image contains a mere five text messages, all of

which are irrelevant. Yet, the CTA knows text messages regarding the issues central to Plaintiff's claims, including his use of the Skeleton Key to access the Dayton RTA BusTime system, exist.

Plaintiff's produced phone image also does not contain other information one would expect to see on an image of cell phone, including: website or search histories; audio or visual files (including photographs); messages sent or received in any third-party applications; or data derived from the vast majority of the third-party applications associated with the cell phone. The CTA is unable to determine the cause of such deficiencies without reimaging the cell phone in its entirety, including all relevant component parts.

The CTA's need to re-image the cell phone is underscored by the fact that the photographs of relevant messages exchanged by Plaintiff and other third parties on his cell phone via the Signal messaging application are completely devoid of affiliated metadata. Without the affiliated metadata, the CTA is unable to verify and authenticate information associated with these messages, including the identity of the sender(s) and the recipient(s) and the dates upon which the messages were sent and received. CTA requested that Plaintiff's production include affiliated metadata (Ex. F) and reiterated the need for messages to be produced in their native formats so that the metadata is preserved and available to the CTA for its review (Ex. D). Accordingly, the CTA is entitled to a complete re-imaging of Plaintiff's phone because that production format will facilitate its review of the requested metadata. *Compare Autotech Techs. Ltd. P'ship v. Automationdirect.com, Inc.*, 248 F.R.D. 556 (N.D. Ill. 2008) (denying motion to compel file structure document in its native format where the party did not request the metadata in its initial request for production).

In *Hespe v. City of Chicago*, Judge Alonso noted that where "the requesting party is able to demonstrate that the responding party has failed in its obligation to search its records and produce the requested information, inspection of the responding party's electronic devices may be

appropriate," especially "when there is a substantiated connection between the device the requesting party seeks to inspect and the claims in the case." 2016 WL 7240754, *4 (N.D. Ill. Dec. 15, 2016). Unlike in *Hespe*, where the defendants were unable to make this showing, *id.* at 5, the CTA here has provided compelling evidence demonstrating that Plaintiff's discovery is incomplete. Plaintiff's obstructive and evasive discovery tactics and refusal to produce relevant discovery over the course of nine months, as well as his most recent attempt to sidestep those shortcomings by producing an incomplete or compromised image of his cell phone, support the CTA's request for inspection and re-imaging of the cell phone that is central to both the claims and counterclaim in this case.

II. Plaintiff should be compelled to respond to the CTA's written discovery requests relating to his personal website.

Plaintiff has failed to produce materials responses to the CTA's request for complete and accurate archived copies of his website, www.menchi.org, and any other websites owned and operated by Plaintiff, as they appeared from May 1, 2018 through the present. Plaintiff objects to this request as "unreasonable," and "harassing." (Ex. M). Plaintiff further claims that his website is not relevant. (*See id.*; Ex. K.)

Plaintiff's objections are meritless. The CTA does not seek this information to harass Plaintiff; it has asserted a defensible basis for seeking these materials under Rule 26. *See* Fed. R. Civ. P. 26 (Parties may obtain discovery regarding any matter that is "relevant to any party's claims or defense" and information "need not be admissible to be discoverable"). Plaintiff's personal website contained detailed and proprietary information about certain CTA technology projects that Plaintiff worked on while employed by the CTA, as recently as October 15, 2020. While that information has since been removed from the site, the CTA is entitled to assess the scope and extent of its proprietary information being shared by Plaintiff in the public domain, as this

information being publicly available raises security concerns for the CTA. The archived copies of this website and any other websites owned and operated by Plaintiff may contain relevant evidence relating to the CTA's affirmative defenses, including unclean hands and after-acquired evidence. The archived websites may also contain admissions or other statements against interest by Plaintiff relevant to this case.

The CTA's request is reasonable. Plaintiff appears to own and operate www.menchi.org (as well as potentially other undisclosed websites). This website is in the public domain, accessible by anyone. It is not unreasonable for Plaintiff to produce the information he is, and has been, making generally available to the public on this (and any other) website, during the relevant time period, including through this litigation, and especially as it relates to his employment at the CTA. Plaintiff is the party best positioned to preserve and produce these materials under his control. Accordingly, the CTA respectfully asks that this Court move to compel Plaintiff to produce complete and accurate archived copies of www.menchi.org, as well as any other personal websites containing discoverable information, as they appeared from May 1, 2018 through the present.

Counsel for Plaintiff denies that Plaintiff deleted any data from his website—despite clear evidence to the contrary—and denies that Plaintiff had an archive of his website as the CTA requested. (Ex. K.) If, as Plaintiff's counsel asserts, Plaintiff has failed to preserve archived versions of www.menchi.org (and any other personal websites), then the CTA respectfully requests that this Court find that Plaintiff has failed to comply with his duty to preserve potentially relevant information. Plaintiff's failure to comply with his discovery obligations is further compounded by the deletion of certain information from his website within the past six weeks. The CTA is unfairly prejudiced by Plaintiff's inability to comply with his discovery obligations. Plaintiff's actions have left the CTA without access or any means to fully evaluate the extent of the information contained

on Plaintiff's website(s) in furtherance of its defenses. If Plaintiff has failed to preserve his website, the CTA asks that the Court find Plaintiff has acted in bad faith and give an adverse-inference instruction. *See* Fed. R. Civ. P. 37(e)(2)(B).

WHEREFORE, the CTA respectfully requests that the Court grant this motion and enter an order compelling Plaintiff to: (i) produce to the CTA his cell phone, along with any and all affiliated SD card(s), and/or storage devices to the CTA for inspection and re-imaging; and (ii) respond to the CTA's Requests for Production relating to his personal website, including by producing complete and accurate archived copies of any personal websites owned or operated by Plaintiff, including but not limited to www.menchi.org, as they appeared from May 1, 2018 through the present. The CTA further respectfully requests this Court order Plaintiff to pay the CTA's expenses incurred in making this motion, including attorney's fees, as provided under Fed. R. Civ. P. 37(a)(5), as well as any other Rule 37 sanction this Court deems appropriate in light of Plaintiff's failure to comply with his discovery obligations, and grant all other relief it deems appropriate.

Dated: February 5, 2021

Respectfully submitted,

CHICAGO TRANSIT AUTHORITY

By: *s/ Elizabeth E. Babbitt*
One of Its Attorneys

John F. Kennedy
jkennedy@taftlaw.com
Elizabeth E. Babbitt
ebabbitt@taftlaw.com
Allison E. Czerniak
aczerniak@taftlaw.com
Nicollette L. Khuans
nkhuans@taftlaw.com
TAFT STETTINIUS & HOLLISTER LLP
111 East Wacker, Suite 2800
Chicago, Illinois 60601
(312) 527-4000

CERTIFICATE OF SERVICE

I hereby certify that on February 5, 2021, the foregoing was filed with the Clerk of Court via CM/ECF, which provided notice of same to all parties who have made an appearance in this case.

s/ *Elizabeth E. Babbitt*